That which is claimed is:

1. A method of rekeying in an authentication system including an authenticated data processing system and an authenticating data processing system, comprising the following carried out by the authenticating data processing system:

detecting failure of an authentication of the authenticated data processing system with a current public key associated with the authenticated data processing system; and

automatically updating the current public key associated with the authenticated data processing system with an updated public key responsive to detecting failure of an authentication of the authenticated data processing system with the current public key.

2. The method of Claim 1, wherein the authentication system comprises a server-side authentication system, the authenticated data processing system comprises an authenticated server and the authenticating data processing system comprises a client of the authenticated server, and wherein detecting failure comprises detecting failure of an authentication of the authenticated server with a current public key associated with the authenticated server; and

wherein automatically updating comprises automatically updating the current public key associated with the authenticated server with an updated public key responsive to detecting failure of an authentication of the authenticated server with the current public key.

3. The method of Claim 2, wherein detecting failure of an authentication of the authenticated server comprises:

receiving a signed certificate from the authenticated server; and

failing to verify the signed certificate with the current public key.

4. The method of Claim 2, wherein automatically updating the current public key associated with the authenticated server comprises:

establishing a connection to an authentication server;

requesting the updated public key from the authentication server over the established connection;

receiving the updated public key over the established connection; and

replacing the current public key at the client with the received updated public key.

5. The method of Claim 4, wherein establishing a connection to the authentication server comprises establishing a secure connection to the authentication server.

6. The method of Claim 3, wherein the secure connection comprises a Secure Sockets Layer encryption only connection.

7. The method of Claim 4, wherein the authenticated server and the authentication server comprise a single server.

8. The method of Claim 4, wherein requesting the updated public key from the authentication server comprises sending a request for an updated public key to the authentication server, the request including an identification of the current public key.

9. The method of Claim 8, wherein the identification of the current public key comprises a checksum of the current public key.

10. The method of Claim 4, wherein receiving the updated public key comprises:

receiving the updated public key signed with a private key corresponding to the current public key; and

verifying a signature of the received signed updated public key with the current public key.

11. The method of Claim 2, wherein the authenticated server comprises a system monitoring server and the client comprises a resource monitoring agent.

12. The method of Claim 1, wherein the authenticated data processing system comprises a client and the authenticated data processing system comprises a server.

13. A method of rekeying in a server-side authentication system including a server, the method comprising the following:

receiving a request for an updated public key from a client over a connection established responsive to the client detecting failure of an authentication of the server by the client; and

providing the updated public key from the server to the client responsive to receiving the request for the updated public key from the client.

14. The method of Claim 13, wherein the connection comprises an encryption only secure connection to the server.

15. The method of Claim 14, wherein the secure connection comprises a Secure Sockets Layer encryption only connection.

16. The method of Claim 13, wherein the request for an updated public key includes an identification of a current public key of the client.

17. The method of Claim 16, wherein the identification of the current public key comprises a checksum of the current public key.

18. The method of Claim 16, further comprising validating the client as authorized to request an updated public key based on the identification of the current public key of the client.

19. The method of Claim 16, further comprising:

selecting a private key from a repository of public/private key pairs based on the identification of the current public key; and

wherein providing the updated public key further comprises:

signing the updated public key utilizing the selected private key; and

sending the signed updated public key to the client over the secure connection.

20. The method of Claim 13, further comprising storing the current public/private key pair of the server in a key repository

21. The method of Claim 20, further comprising signing an authentication certificate of the server with the updated private key.

22. The method of Claim 13, wherein the client further carries out the following:

automatically requesting updating of the current public key of the client associated with the server with an updated public key responsive to detecting failure of an authentication of the server with the current public key.

23. The method of Claim 22, wherein the client detecting failure of an authentication of the server comprises:

receiving a signed certificate from the server; and

failing to verify a signature of the signed certificate with the current public key.

24. The method of Claim 22, further comprising the client carrying out the following:

receiving the updated public key from the server; and

replacing the current public key with the updated public key.

25. The method of Claim 24, wherein receiving the updated public key comprises:

receiving the updated public key signed with a private key corresponding to the current public key; and

verifying a signature of the received signed updated public key with the current public key.

26. The method of Claim 13, wherein the server comprises a system monitoring server and the client comprises a resource monitoring agent.

27. A system for rekeying a server-side authentication system, comprising:

a first client configured to detect failure of the first client to authenticate an authenticated server and to automatically request an updated public key associated with the authenticated server for which authentication failure was detected; and

an authentication server configured to receive requests for updated public keys from the first client and send updated public keys to the first client.

28. The system of Claim 27, further comprising a key repository operably associated with the authentication server, the key repository being configured to store previous public/private key pairs associated with the authenticated server.

29. The system of Claim 28, wherein the authentication server is further configured to select a public/private key pair from the key repository corresponding to a current public key of the first client from which a request was received and sign the updated public key with a private key of the selected public/private key pair.

30. The system of Claim 29, wherein the first client is further configured to receive the updated public key from the authentication server and to verify a signature of the received updated public key with the current public key of the first client.

31. The system of Claim 29, further comprising a second client configured to detect failure of the second client to authenticate an authenticated server and automatically request an updated public key associated with the authenticated server for which authentication failure was detected; and

wherein the authentication server is further configured to receive requests for updated public keys from the second client and send updated public keys to the second client.

32. The system of Claim 31, wherein the authentication server is further configured to select a public/private key pair from the key repository corresponding to a current public key of the first client from which the request was received and sign the updated public key with a private key of the selected public/private key pair and to select a public/private key pair from the key repository corresponding to a current public key of the second client from which the request was received and sign the updated public key with a private key of the selected public/private key pair.

33. The system of Claim 32, wherein the selected public/private key pair from the key repository corresponding to a current public key of the second client and the selected public/private key pair from the key repository corresponding to a current public key of the first client are different public/private key pairs.

34. An authenticating data processing system for use in a system for rekeying in an authentication system including an authenticated data processing system, comprising:

means for detecting failure of an authentication of the authenticated data processing system with a current public key associated with the authenticated data processing system; and

means for automatically updating the current public key associated with the authenticated data processing system with an updated public key responsive to detecting failure of an authentication of the authenticated data processing system with the current public key.

35. The authenticating data processing system of Claim 34, wherein the authentication system comprises a server-side authentication system, the authenticating data processing system comprises a client and the authenticated data processing system comprises a server.

36. A computer program product for rekeying in an authentication system including an authenticating data processing system and an authenticated data processing system, the computer program product comprising:

a computer readable medium having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code configured to detect failure of an authentication of the authenticated data processing system with a current public key associated with the authenticated data processing system; and

computer readable program code configured to automatically update the current public key associated with the authenticated data processing system with an updated public key responsive to detecting failure of an authentication with the current public key.

37. The computer program product of Claim 36, wherein the authentication system comprises a server-side authentication system, the authenticating data processing system comprises a client and the authenticated data processing system comprises a server.

38. A method of rekeying in an authentication system having an authenticated communication, comprising the following carried out by an authenticating data processing system:

detecting failure of an authentication of an authenticated communication with a current public key associated with a source of the authenticated communication; and

automatically updating the current public key associated with the source of the authenticated communication with an updated public key responsive to detecting failure of an authentication of the authenticated communication with the current public key.

39. The method of Claim 38, wherein the authenticated communication comprises a signed certificate, the authenticating data processing system comprises a client and the source of the authenticated communication comprises a server.

40. The method of Claim 38, wherein the authenticated communication comprises a signed certificate, the authenticating data processing system comprises a server and the source of the authenticated communication comprises a client.

41. The method of Claim 38, wherein the authenticated communication comprises an e-mail message, wherein the authenticating data processing system comprises a mail recipient and the source of the authenticated communication comprises a source of the e-mail message.

42. The method of Claim 41, wherein the source of the e-mail message comprises an author of the e-mail.

43. The method of Claim 41, wherein the source of the e-mail message comprises an e-mail server.